Is there a Universally Accepted Narrative for CAI (Cyber AI) ? Lets See.

General Definition :

Computerised System that exhibits behaviour that is commonly thought of as requiring Intelligence or A System Capable of rationally solving complex problems or taking appropriate Actions to achieve its goals in whatever real world circumstances it encounters.

In 2016 Google CEO Sundar Pichai said – "ML (A sub field of AI is a core , transformative way by which we are rethinking how we are doing everything . We are thoughtfully applying it across all our products be it search ads , Youtube , or Play . And we are in Early days but you will see us in a systematic way apply ML in all these areas."

Now Fast forward to 2023 – Witness the Evolution of Google BARD while passing through DEEP MIND.
And the Phenomenon/Revolution called OpenAI's ChatGpt .

Experts offer different Taxonomies for AI Problems and Solutions . Here's my favourite One from AI Textbook by Stuart Russell and Peter Norvig (AI Modern Approach 3rd Edition. Essex , England : Pearson , 2009).

1. Systems that think like Humans (Cognitive Architectures & Neural Networks).
2. Systems that act like Humans (Pass the Turing test via natural language processing,knowledge representation,automated reasoning and Learning)
3. Systems that think Rationally (Logic solvers , inference and optimization).
4. Systems that Act Rationally (Intelligent software agents and embodied robots that achieve goals via perception , planning , reasoning , learning , communication , decision making and acting)

Do we Humans really represent or demonstrate the above traits in Technical terms during peace time and duress ? On the Contrary the combination of above can be " A Humans Envy "

Venture Capitalist Frank Chen broke down AI into 5 Categories – Logical Reasoning , Knowledge Representation , Planning and Navigation , Natural Language processing and perception.

AI Researcher Pedro Domingos ascribed AI Researchers to 5 Tribes based on the methods they use.

1. Symbolists – use logical reasoning based on abstract symbols.
2. Connectionists – Build structures inspired by human brain.
3. Evolutionaries - use methods inspired by Darwinian evolution.
5. Bayesians – Use probabilistic inference.
6. Analogizers – extrapolate from similar cases seen previously.

Today Big Data Algorithms and Systems are analysing massive volumes of data at great speed and scale.

Boundaries of AI can be uncertain and have shifted over time. Solutions identified become part of routine data processing. Core objective of AI Research and application has always been to automate and replicate intelligent behaviour.

AI on Smartdevice & Handhelds (Succinctly)

Attributes Power Combination = Logic , Reasoning ,Conceptualisation , self awareness , learning , emotional knowledge , Planning , Creativity , abstract thinking , Problem solving.
SELF SENTIENCE BEING

DNN (Deep Neural Networks) - Machine Learning (ML) – Inference & Training on Cloud based ML servers.
Eg - Speech & Image recognition

Additional Benefits.

Latency – Local Inference delivers quicker Results.

Myraid Privacy & Security Advantages when data not transferred over the Cloud.

On device inference (Locally) .
Eg – Latest Gen Smartphone ARM Processor with AI Engine.
Efficient = Saves Network Bandwidth , saves power on device(Mobile Radios 5G Wifi non operational) & Server room (No Processing)

Advantages :
Update Neural Networks with better models by service providers.

Dedicated Hardware with less power & thermal constraints can run deep & complex models.

“ While the Cloud has allowed ML to enter mainstream – The Real Power of ML will come from Distributed Decentralised Intelligence when devices combo together with Cloud Servers “ - AND DURING CONTINGENCIES / RADIO SATCOM Silence...in Isolation or through Mesh Capability (Edge Computing Inputs). #later in presentation.

AI Augmented Device capability & Experience is limitless.

Era of Heterogeneous Computing – DNN Inference through CPU GPU DSP – Different Hardware yields different performance & Power Efficiency.

The software side of most AI Engines today are Agnostic – support for most popular frameworks like Tensorflow caffee2. Today Specialised Libraries can run DNN’s on Hexagon DSP’s taking advantage of Hexagon Vector eXtensions (HVX)

IN A NUTSHELL – Improved Visual & Audio Intelligence with Greater Privacy. AI is indeed transforming everything . Making on Device AI Ubiquitous.

AI impact on cybersecurity -

AI Cyberdefense systems are being implemented to proactively detect and mitigate threats. Traditional antivirus relies on blacklisting historic threats based on virus signatures. AI based EDR can recognise aspects of software that may be malicious without the need to rely on pre defined database.

MAJOR APPLICATION IN -

EDR - USER AUYHENTICATION - NETWORK DETECTION - INTRUSION DETECTION AND PREVENTION (IDS) - LOG MANAGEMENT AND SIEM.

Behavioural Biometrics identifies users based on unique aspects of their digital activity - Active authentication systems enhance cybersecurity by ensuring ongoing user authentication

CYBER AI 4 ZERO TRUST NETWORK ACCESS (ZTNA) - Intelligent dynamic multi dimensional security approach.

Smart Automation for the complete process. Real time monitoring 2 identify breaches (Alarm React Respond). Intelligent Behavioural Analytics to identify patterns - Erratic Actions through combination of user data + location + user behaviour = Log info 4 future access reference retrieval. If APT breach identified mechanically protect the centralised data vault.

Behavioural Analytics .

Application of complex algorithms to individual level data to derive insights , generate forecasts and make predictions about future human behaviour. Global INTEL Agencies could hypothetically implement AI to make predictions about future behaviour. Major Application - Insider Threat Detection (ITD) - Govt & Military etc.
BA is here to stay. BA techniques may not just be effective in refining assessment of risk but also discovering new leads about evolving cyber threats landscape. Increasingly sophisticated use of AI and BA can be deployed to extract information from bulk datasets.

US Pentagon believes that precognitive AI can predict events 'days in advance' - Global Information Dominance Experiments (GIDE) - AI + CLOUD COMPUTING + SENSORS. Mix of military and civilian sensors to address scenarios where contested logistics might pose a problem. GIDE tech employs ML based system to send fast critical updates and alerts. Can prevent surprise aggression or lead to negotiations instead of conflict . Humans will still be heavily involved in the process.

Complex weapons platforms also coordinate attack or defense among geographically disparate forces. A CyberAttack on these weapons platforms can crash the software used to runthem. That could sideline a fighter jet or radar that protects a aircraft carrier battlegroup or cause a Military satellite to go offline using non kinetic means . Satellite navigation systems are also at risk of jamming and spoofing. Satellites are also crucial for coordinating electricity grids and time stamping financial transactions. Geolocation is susceptible to electronic interference.

Penetrating communication networks , sabotaging databases (deleting spare engines for fighter jets from spare parts roster) and locking legitimate users out from crucial networks. The NSA wants military industrial complex to take cyber vulnerabilities seriously. Unlike the kinetic battlefield where aircraft drones and armored fighting vehicles spend most of their time out of contact with the enemy - The wireless nature of computer networks means that those same weapons will be under constant threat of enemy assault . And that requires a different kind of armor.

credit - NATIONAL SECURITY AGENCY.

A Supply chain attack is an incredibly expensive operation . Back doors imitate legimitate email users and fool the electronic systems that are supposed to assure identities of users with the right login credentials and additional authentication. Such an attack has the opportunity to hit a massive quantity of targets but if reached to far the APT would lose their incredible access - FireEye

Complex Weapon systems and platforms are vulnerable to Cyber Attack - Weapon Systems don't just include hypersonic missiles or lasers. There are computers at wings , at sea and on land. We don't think of weapons systems that way but none of them works without computers.These computers add functionality , including fire control (correcting and adjusting aim against distant or fast moving targets), navigation,(receiving AGPS signals) and communications (voice and data).

UN Appointed independent rights experts - AI Powered spyware & disinformation is on the rise & regulation of Space has become urgent.AI based biometric surveillance systems are increasingly being used in sensitive contexts without individuals knowledge or consent. Urgent & strict regulatory red lines are needed for technologies that claim to perform emotion or gender recognition. The Human Rights Council appointed experts condemned the already alarming use and impacts of spyware and surveillance technologies on the work of human rights defenders and journalists often under the guise of National security and counter terrorism measures

Human Rights Council also called for regulation to address the lightning fast development of generative AI that's enabling mass production of fake online content which spreads disinformation and hate speech. Encryption and Privacy are paramount. They underlined the need to ensure technical solutions - including strong end to end encryption and unfettered access to VPNs - and secure and protect digital communications.

"Adversarial AI" - A Threat to military systems - Shift5's Lospinoso says - The former Army Captain told a Senate Armed Services panel how AI can impact Military Operations.

"Adversarial AI" - A Threat to military systems - Shift5's Lospinoso says - The former Army Captain told a Senate Armed Services panel how AI can impact Military Operations.

AI for cybersecurity and cybersecurity for AI.

AI in cybersecurity presents great opportunities but as with any powerful general purpose dual use technology , it also brings great challenges. AI can improve cybersec and defence measures allowing for greater system robustness , resilience and responsiveness but AI in the form of ML and deep learning will escalate sophisticated cyberattacks enabling faster and better targeted and more destructive attacks.

The application of AI in cybersecurity also poses security and ethical concerns. Among other things it remains unclear to see how responsibilities for autonomous response systems should be ascribed. How to make sure systems are behaving according to expectations. Or what the security risks carried by the increasing anthropomorphisation of AI systems are. ANTHROPOMORPHIC LANGUAGE AT TIMES APPEARS INTRINSIC TO THE FIELD OF AL RESEARCH

The Organisation for economic cooperation and development (OECD) defines an AI system as a "machine based system that can for a given set of human defined objectives make predictions recommendations or decisions influencing real or virtual environments." This definition has also been accepted and adopted by the European Commission in the Regulation on a European approach for AI.

ML is a set of techniques to allow machines to learn in an automated manner through patterns and inferences rather than through explicit instructions through a human. ML approaches often teach machines to reach an outcome by showing them many examples of correct outcomes. However they can also define a set of rules and let the machine learn by trail and error.

Neural networks involve repeatedly interconnecting thousands or millions of simple transformations into a larger statistical machine that can learn sophisticated relationships between inputs and outputs Neural networks modify there own code to find and optimise links between inputs and outputs

Deep learning is a large neural network subset composed of hierarchical layers that increase the complexity of the relationships between input and output.

AI in cybersecurity can be identified in 3 categories. - Detection 51% Prediction 34% and response 18%.

Driving forces that are boosting the use of AI in cybersecurity.

1. Speed of impact – in some of the major attacks the average time of impact on the organisation is 4 mins. Todays attacks are not just ransomware or just targeting certain systems or vulnerabilities they can move and adjust based on what the targets are doing. These kind of attacks impact incredibly quickly and there are not many human interactions that can happen in the meantime.

2. Operational complexity. - Today the proliferation of cloud computing platforms and the fact that those platforms can be operationalised and deliver services quickly in the milliseconds range. Means that you cannot have a lot of humans in that loop and you have to think about a more analytics driven capability.

3. Skills gap – There is a global shortage of about a million and a half cybersecurity professionals. This level of scarcity pushes the industry to automate at a faster rate.

AI can help security teams in 3 ways. - By improving systems robustness response and resilience ...The 3R model.

AI can improve systems robustness that is the ability of a system to maintain its initial assumed stable configuration even when it processes erroneous inputs. Thanks to self testing and self healing software. This means that AI systems can be used to improve testing for robustness delegating to the machines the process of verification and validation.

AI can strengthen systems resilience – the ability of a system to resist and tolerate an attack by facilitating threat and anomaly detection.

AI can be used to enhance response – the capacity of a system to respond autonomously to attacks , to identify vulnerabilities in other machines and to operate strategically by deciding which vulnerability to attack and to launch more aggressive counterattacks.

Identifying when to delegate decision making and response actions to AI and the need of an individual org to perform risk impact assessment are related. In many cases AI will augment without replacing the decision making of human security analysts and will be integrated into the process that accelerate response times.